VIRUS INVESTIGATION FORM
(Fax Attn: Andrew Cooke 301-903-0746)

INVESTIGATION FORMS MUST BE RETURNED TO VIRUS COORDINATOR WITHIN 1 DAY OF RESPONSE.

SECTION 1: GENERAL INFORMATION

Incident #: Date:

User: Org.:

ViRT Member:

Arrival Time: Departure Time:

On-site symptoms (circle one):

DOEVStop detected Norman (SBB) detected

Cat-s Claw detected Norton detected

McAfee detected Recipient of infected email

E-mail gateway detected System would not boot

Other:_____

_____

_____

Antivirus software installed Yes No

Package:_____ Version:_____

If NO, did you install? Yes No

If outdated, did you update? Yes

No

Software used for eradication (circle one):

Boot Sector: DOEVFix Norman Norton McAfee VirHunt

File Infector: Norman Norton McAfee VirHunt Deleted

Macro: Norman Norton McAfee Deleted

Other:_____

Virus Name:_____
(If more than one virus found, create separate incidents for each.)

Virus Type (refer to DOE Virus List for confirmation):

Macro Virus: _____ (Fill out Sections 2 & 4)

Boot Sector Virus: _____ (Fill out Sections 3 & 4)

Application Infector: _____ (Fill out Sections 2 & 4)

Multipartite: _____ (Fill out Sections 3 & 4)

Is the virus a known DOE virus (is it on the latest DOE Virus List)?

Yes No Date of Virus List:

(If NO, page the ASSIST immediately at (202) 539-3808. Obtain copy of diskette (boot sector) or data file (macro).)

Is the virus destructive (refer to DOE Virus List)?

Yes No

(If YES, page the ASSIST immediately at (202) 539-3808.)

SECTION 2: MACRO/APPLICATION VIRUS INFECTIONS

Was the infected file sent via e-mail? Yes No

If possible, print message (address list), attach, and answer the following questions.

If the infected file was not sent via email, where did it come from (answer questions 1-5)?

1. Who was the sender?

_____

2. Who else received it?_____

_____

_____

3. Has the sender been notified of the virus? Yes No

By whom (circle one)? User ViRT

4. Have recipients outside of HQ been notified? Yes No

By whom (circle one)? User ViRT

5. Have recipients within DOE been visited? Yes No

Number of infected files:

If possible, attach list of infected files with file dates and times (e.g., use DIR > LPT1: to list, then mark appropriate files.)

Was NORMAL.DOT infected? Yes No

NORMAL.DOT file date/time:_____
(prior to virus eradication)

Location of NORMAL.DOT. ___Server ___ Hard drive

Was application infector located on server? Yes No

(If SERVER or Yes, page the ASSIST immediately at (202) 539-3808 and notify server Administrator.)

SECTION 3: BOOT SECTOR VIRUS INFECTIONS

Number of diskettes infected:_____

Were infected diskettes used in other DOE systems?

Yes No

If yes, user name: Room :

Were they contacted? Yes No

Number of systems infected:_____

If the system was infected, why did the user boot from diskette?

_____

_____

_____

Who provided the diskette?

_____

Has the provider been notified of the virus? Yes No

By whom (circle one)? User ViRT

Who else received or used the diskette?_____

_____

Have users been notified? Yes No

By whom (circle one)? User ViRT

POTENTIAL QUESTIONS FOR BOOT SECTOR INFECTIONS:

Does anyone else use the system? [ ] Yes [ ] No If yes, whom?_____
Have you recently received diskettes from anyone? [ ] Yes [ ] No If yes, whom?
_____
Have you recently given diskettes to anyone? [ ] Yes [ ] No If yes, who?_
Do you share diskettes between home and work? [ ] Yes [ ] No
Is your home system protected against viruses? [ ] Yes [ ] No Package?___
Have you used other systems at DOE, Colleges, End User Center, etc.. [ ] Yes [ ] No Where?____
Has AOSS Support Team or Hardware Tech. performed work on PC lately? [ ] Yes [ ] No
Who?_____ When?__
Have you ever had a virus before? [ ] Yes [ ] No When?____

SECTION 4: RESOLUTION INFORMATION

SOURCE

___DOE Field Site Name of Site:

___Gov=t Agency Name of Agency:

___Outside Contractor Name of Person/Co.:

___Civic Organization Name of Organization:

___School/University Name of School:

___DOE Travel Location:

___Internal User.Org.:

___Home PC ___Personal Friend

___Prior Infection ___False Alarm

___Other (be specific):_____

Source notified by: User ViRT

Other:_____

Notes:

FOLLOW-UP

AOSS Support Contacted?

Yes No

Name:_____

Phone #:_____

NOTES

Provide additional information here. It is important to describe how each media item (file, diskette, system) became infected. A complete history of the virus spread, from source to all affected parties within DOE, must be provided, including resolution of all system examinations. For simple encounters (virus detected immediately on protected system, no other DOE recipients, and no spread to other users), information in previous sections should be sufficient.